VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
ACDPA5003PWO		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/DE 00/ 03507	05/10/2000	07/10/1999
Anmelder		
DEUTSCHE POST AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 4 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [ ] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [X] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 2

   [X] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

Feld III **WORTLAUT DER ZUSAMMENFASSUNG (Fortsetzung von Punkt 5 auf Blatt 1)**

Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls, das ein temporäres, einem Dokumenthersteller unbekanntes, Geheimnis erzeugt das zusammen mit der Identität des Sicherungsmoduls verschlüsselt an eine Bescheinigungsstelle übergeben wird, die das temporäre Geheimnis entschlüsselt. Die Bescheinigungsstelle erkennt die Identität des Sicherungsmoduls und verschlüsselt das temporäre Geheimnis zusammen mit weiteren Informationen derart, dass nur eine Prüfstelle sie entschlüsseln kann. Die Bescheinigungsstelle übermittelt die Informationen an den Dokumenthersteller, der eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt. Das Sicherungsmodul verknüpft die selbst vom Dokumenthersteller eingebrachten Daten mit dem temporären Geheimnis irreversibel, so dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann. Das Ergebnis der irreversiblen Verknüpfung der Daten mit dem temporären Geheimnis wird in das Dokument übernommen.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
T/DE 00/03507

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07B17/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
PAJ, WPI Data, INSPEC, EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 0 331 352 A (ALCATEL BUSINESS SYSTEMS ;ALCATEL NV (NL)) 6. September 1989 (1989-09-06) Spalte 1, Zeile 1 - Zeile 5 Spalte 2, Zeile 8 - Zeile 45 Spalte 4, Zeile 34 -Spalte 5, Zeile 5 Spalte 6, Zeile 10 - Zeile 21 ---	1-9
Y	AKL S G ET AL: "DIGITAL SIGNATURES: A TUTORIAL SURVEY" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, Bd. 16, Nr. 2, Februar 1983 (1983-02), Seiten 15-24, XP000946230 ISSN: 0018-9162 Seite 19, rechte Spalte -Seite 23, linke Spalte ---	1-9
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12. Dezember 2001	09/01/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

3

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,A	HUHNLEIN D ; MERKLE J : "Secure and cost efficient electronic stamps " SECURE NETWORKING - CQRE SECURE'99, PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.1740), 'Online! 30. November 1999 (1999-11-30) - 2. Dezember 1999 (1999-12-02), Seiten 94-100, XP002185463 Dusseldorf, Germany ISBN: 3-540-66800-4 Gefunden im Internet: <URL:http://citeseer.nj.nec.com/cs> 'gefunden am 2001-12-12! das ganze Dokument	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
T/DE 00/03507

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0331352 A	06-09-1989	AT 107057 T	15-06-1994
		DE 68915816 D1	14-07-1994
		DE 68915816 T2	19-01-1995
		EP 0331352 A2	06-09-1989
		US 4934846 A	19-06-1990

PTO/PCT Rec'd 02 APR 2002

PCT

Receiving Office Request Form POST-2
(5) pages

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen

Internationales Anmeldedatum

Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)* ACDPA5003PWO

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren zur Erstellung und Überprüfung fälschungssicherer Dokumente

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

DEUTSCHE POST AG
Heinrich-von-Stephan-Straße 1

D-53175 Bonn

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat): Deutschland

Sitz oder Wohnsitz (Staat): Deutschland

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

LANG, Jürgen
Schau ins Land 15

D-51429 Bergisch Gladbach

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): Deutschland

Sitz oder Wohnsitz (Staat): Deutschland

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☒ Anwalt ☐ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

JOSTARNDT, Hans-Dieter
Eupener Straße 266

D-52076 Aachen
Deutschland

Telefonnr.: (++49)241/54 32 13

Telefaxnr.: (++49)241/543240

Fernschreibnr.:

☐ Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Blatt Nr. 2

Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Wird keines der folgenden Felder benutzt, so ist dieses Blatt dem Antrag nicht beizufügen.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

MEYER, Bernd
Zum Stöckerhof 2 c

D-53639 Königswinter

Diese Person ist:
☐ nur Anmelder
☒ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): Deutschland
Sitz oder Wohnsitz (Staat): Deutschland

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):
Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):
Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):
Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

- ☒ AP **ARIPO-Patent:** GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☒ EA **Eurasisches Patent:** AM Armenien, AZ Aserbaidschan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ EP **Europäisches Patent:** AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, DE Deutschland, DK Dänemark, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☒ OA **OAPI-Patent:** BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

- ☒ AL Albanien .....
- ☒ AM Armenien .....
- ☒ AT Österreich .....
- ☒ AU Australien .....
- ☒ AZ Aserbaidschan
- ☒ BA Bosnien-Herzegowina .....
- ☒ BB Barbados
- ☒ BG Bulgarien .....
- ☒ BR Brasilien .....
- ☒ BY Belarus
- ☒ CA Kanada
- ☒ CH und LI Schweiz und Liechtenstein
- ☒ CN China .....
- ☒ CU Kuba .....
- ☒ CZ Tschechische Republik .....
- ☒ DE Deutschland .....
- ☒ DK Dänemark .....
- ☒ EE Estland .....
- ☒ ES Spanien .....
- ☒ FI Finnland .....
- ☒ GB Vereinigtes Königreich
- ☒ GE Georgien .....
- ☒ GH Ghana .....
- ☒ GM Gambia
- ☒ GW Guinea-Bissau .....
- ☒ HU Ungarn .....
- ☒ ID Indonesien
- ☒ IL Israel .....
- ☒ IS Island
- ☒ JP Japan .....
- ☒ KE Kenia .....
- ☒ KG Kirgisistan .....
- ☒ KP Demokratische Volksrepublik Korea .....
  .....
- ☒ KR Republik Korea .....
- ☒ KZ Kasachstan .....
- ☒ LC Saint Lucia
- ☒ LK Sri Lanka
- ☒ LR Liberia
- ☒ LS Lesotho .....
- ☒ LT Litauen
- ☒ LU Luxemburg
- ☒ LV Lettland
- ☒ MD Republik Moldau .....
- ☒ MG Madagaskar .....
- ☒ MK Die ehemalige jugoslawische Republik Mazedonien .....
- ☒ MN Mongolei
- ☒ MW Malawi .....
- ☒ MX Mexiko .....
- ☒ NO Norwegen
- ☒ NZ Neuseeland .....
- ☒ PL Polen .....
- ☒ PT Portugal .....
- ☒ RO Rumänien
- ☒ RU Russische Föderation .....
- ☒ SD Sudan
- ☒ SE Schweden
- ☒ SG Singapur
- ☒ SI Slowenien .....
- ☒ SK Slowakei .....
- ☒ SL Sierra Leone
- ☒ TJ Tadschikistan .....
- ☒ TM Turkmenistan .....
- ☒ TR Türkei .....
- ☒ TT Trinidad und Tobago .....
- ☒ UA Ukraine .....
- ☒ UG Uganda .....
- ☒ US Vereinigte Staaten von Amerika .....
  .....
- ☒ UZ Usbekistan .....
- ☒ VN Vietnam .....
- ☒ YU Jugoslawien .....
- ☒ ZW Simbabwe .....

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☒ .....
- ☐ .....
- ☐ .....

Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der Bestimmung von _____.

Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

Siehe Anmerkungen zu diesem Antragsformular

Feld Nr. VI PRIORITÄTSANSPRUCH Weitere Prioritätsansprüche sind im Zusatzfeld angegeben. ☐

Die Priorität der folgenden früheren Anmeldung(en) wird hiermit beansprucht:

Staat (Anmelde- oder Bestimmungsstaat der Anmeldung)	Anmeldedatum (Tag/Monat/Jahr)	Aktenzeichen	Anmeldeamt (nur bei regionaler oder internationaler Anmeldung)
(1) Deutschland	27.04.2000 (27. April 2000)	100 20 563.1-31	
(2) Deutschland	07.10.1999 (07. Oktober 1999)	199 48 319.1	
(3)			

Dieses Kästchen ankreuzen, wenn die beglaubigte Kopie der früheren Anmeldung von dem Amt ausgestellt werden soll, das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist (eine Gebühr kann verlangt werden):

☒ Das Anmeldeamt wird hiermit ersucht, eine beglaubigte Abschrift der oben in Zeile(n) 1,2 bezeichneten früheren Anmeldung(en) zu erstellen und dem Internationalen Büro zu übermitteln.

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der Internationalen Recherchenbehörde (ISA *(Sind zwei oder mehr Internationale Recherchenbehörden für die internationale Recherche zuständig, ist der Name der Behörde anzugeben, die die internationale Recherche durchführen soll; Zweibuchstaben-Code genügt)*: ISA/ _____

Frühere Recherche *Auszufüllen, wenn eine Recherche (internationale Recherche, Recherche internationaler Art oder sonstige Recherche) bereits bei der Internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist und diese Behörde nun ersucht wird, die internationale Recherche soweit wie möglich auf die Ergebnisse einer solchen früheren Recherche zu stützen. Die Recherche oder der Recherchenantrag ist durch Angabe der betreffenden Anmeldung (bzw. deren Übersetzung) oder des Recherchenantrags zu bezeichnen.*

Staat (oder regionales Amt): Datum *(Tag/Monat/Jahr)*: Aktenzeichen:

Feld Nr. VIII KONTROLLISTE

Diese internationale Anmeldung umfaßt:

1. Antrag	: 4	Blätter
2. Beschreibung	: 15	Blätter
3. Ansprüche	: 3	Blätter
4. Zusammenfassung	: 1	Blätter
5. Zeichnungen	: 2	Blätter
Insgesamt	: 25	Blätter

Dieser internationalen Anmeldung liegen die nachstehend angekreuzten Unterlagen bei:

1. ☐ Unterzeichnete gesonderte Vollmacht
2. ☐ Kopie der allgemeinen Vollmacht
3. ☐ Begründung für das Fehlen der Unterschrift
4. ☐ Prioritätsbeleg(e) *(durch die Zeilennummer von Feld Nr. VI kennzeichnen)*:
5. ☒ Blatt für die Gebührenberechnung
6. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen
7. ☐ Sequenzprotokolle für Nucleotide und/oder Aminosäuren (Diskette)
8. ☐ Sonstige *(einzeln aufführen)*:

Abbildung Nr. 2 der Zeichnungen (falls vorhanden) soll mit der Zusammenfassung veröffentlicht werden.

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Dr. Hans-Dieter Jostarndt
- Patentanwalt -

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:
2. Zeichnungen ☐ eingegangen: ☐ nicht eingegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:
5. Vom Anmelder benannte Internationale Recherchenbehörde: ISA/
6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Dieses Blatt ist nicht Teil und zählt nicht als Blatt der internationalen Anmeldung.

PCT

BLATT FÜR DIE GEBÜHRENBERECHNUNG
Anhang zum Antrag

Von Anmeldeamt auszufüllen

Internationales Aktenzeichen

Eingangsstempel des Anmeldeamts

Aktenzeichen des Anmelders oder Anwalts: ACDPA5003PWO

Anmelder: DEUTSCHE POST AG, Heinrich-von-Stephan-Straße 1, D-53175 Bonn

BERECHNUNG DER VORGESCHRIEBENEN GEBÜHREN

1. ÜBERMITTLUNGSGEBÜHR . . . . . 175,00 T

2. RECHERCHENGEBÜHR . . . . . 1848,26 S

Die internationale Recherche ist durchzuführen von _____
(Sind zwei oder mehr Internationale Recherchenbehörden für die internationale Recherche zuständig, ist der Name der Behörde anzugeben, die die internationale Recherche durchführen soll.)

3. INTERNATIONALE GEBÜHR

Grundgebühr
Die internationale Anmeldung enthält 25 Blätter.

umfaßt die ersten 30 Blätter . . . . . 799,93 b_1

_____ x _____ = _____ b_2
Anzahl der Blätter über 30 — Zusatzblattgebühr

Addieren Sie die in Feld b_1 und b_2 eingetragenen Beträge, und tragen Sie die Summe in Feld B ein . . . . 799,93 B

Bestimmungsgebühren
Die internationale Anmeldung enthält 8 Bestimmungen.

172,11 x 8 = 1376,88 D
Anzahl der zu zahlenden Bestimmungsgebühren *(maximal 11)* — Bestimmungsgebühr

Addieren Sie die in Feld B und D eingetragenen Beträge, und tragen Sie die Summe in Feld I ein . . . . . 2176,81 I
(Anmelder aus einigen Staaten haben Anspruch auf eine Ermäßigung der internationalen Gebühr um 75%. Hat der Anmelder (oder haben alle Anmelder) einen solchen Anspruch, so beträgt der in Feld I einzutragende Gesamtbetrag 25% der Summe der in Feld B und D eingetragenen Beträge.)

4. GEBÜHR FÜR PRIORITÄTSBELEG . . . . . 56,00 P

5. GESAMTBETRAG DER ZU ZAHLENDEN GEBÜHREN
Addieren Sie die in Feldern T, S, I und P eingetragenen Beträge, und tragen Sie die Summe in das nebenstehende Feld ein 4256,07
INSGESAMT

☐ Die Bestimmungsgebühren werden jetzt noch nicht gezahlt.

ZAHLUNGSWEISE

☒ Abbuchungsauftrag (siehe unten) ☐ Bankwechsel ☐ Kupons
☐ Scheck ☐ Barzahlung ☐ Sonstige *(einzeln angeben):*
☐ Postanweisung ☐ Gebührenmarken

ABBUCHUNGSAUFTRAG *(diese Zahlungsweise gibt es nicht bei allen Anmeldeämtern)*

Das Anmeldeamt/ DPA

☒ wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen.

☒ wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben.

☒ wird beauftragt, die Gebühr für die Ausstellung des Prioritätsbelegs und seine Übermittlung an das Internationale Büro der WIPO von meinem laufenden Konto abzubuchen.

3 410 651 00 — Kontonummer

04. Oktober 2000 — Datum *(Tag/Monat/Jahr)*

Unterschrift

Siehe Anmerkungen zum Blatt für die Gebührenberechnung

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

JOSTARNDT, Thul
Brüsseler Ring 51
52074 Aachen
ALLEMAGNE

Date of mailing (day/month/year)
14 février 2002 (14.02.02)

Applicant's or agent's file reference
ACDPA5003PWO

IMPORTANT NOTIFICATION

International application No.
PCT/DE00/03507

International filing date (day/month/year)
05 octobre 2000 (05.10.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address
JOSTARNDT, Hans-Dieter
Eupener Strasse 266
52076 Aachen
Germany

State of Nationality:
State of Residence:
Telephone No.: 49 241 54 32 13
Facsimile No.: 49 241 54 32 40
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address
JOSTARNDT, Thul
Brüsseler Ring 51
52074 Aachen
Germany

State of Nationality:
State of Residence:
Telephone No.: 49 241 400 71 00
Facsimile No.: 49 241 400 71 21
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Alison OSBORNE

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

004664735

[redacted]

Der Antrag ist bei der zuständigen mit der internationalen vorläufigen Prüfung beauftragten Behörde oder, wenn zwei oder mehr Behörden zuständig sind, bei der vom Anmelder gewählten Behörde einzureichen. Der Anmelder kann den Namen oder den Zweibuchstaben-Code der Behörde auf der nachstehenden Zeile angeben.

IPEA/ _____

PCT/IPEA/401 (4) pages

PCT

KAPITEL II

POST-2

ANTRAG AUF INTERNATIONALE VORLÄUFIGE PRÜFUNG

nach Artikel 31 des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens:
Der (die) Unterzeichnete(n) beantragt (beantragen), daß für die nachstehend bezeichnete internationale Anmeldung die internationale vorläufige Prüfung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens durchgeführt wird.

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

Bezeichnung der IPEA	Eingangsdatum des ANTRAGS

Feld Nr. I KENNZEICHNUNG DER INTERNATIONALEN ANMELDUNG		Aktenzeichen des Anmelders oder Anwalts: ACDPA5003PWO
Internationales Aktenzeichen: PCT/DE00/03507	Internationales Anmeldedatum *(Tag/Monat/Jahr)*: 05. Oktober 2000 (05.10.2000)	(Frühester) Prioritätstag *(Tag/Monat/Jahr)*: 07. Oktober 1999 (07.10.1999)
Bezeichnung der Erfindung: Sicherungsmodul und Verfahren zur Erstellung fälschungssicherer Dokumente		

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*	Telefonnr.:
DEUTSCHE POST AG Heinrich-von-Stephan-Straße 1 D-53175 Bonn	Telefaxnr.:
	Fernschreibnr.:

Staatsangehörigkeit (Staat):	Sitz oder Wohnsitz (Staat):
Deutschland	Deutschland

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*
LANG, Jürgen Schau ins Land 16 D-51429 Bergisch Gladbach

Staatsangehörigkeit (Staat):	Sitz oder Wohnsitz (Staat):
Deutschland	Deutschland

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*
MEYER, Bernd Zum Stöckerhof 2 c D-53639 Königswinter

Staatsangehörigkeit (Staat):	Sitz oder Wohnsitz (Staat):
Deutschland	Deutschland

☐ Weitere Anmelder sind auf einem Fortsetzungsblatt angegeben.

Internationales Aktenzeichen
PCT/DE00/03507

Feld Nr. III ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT

Die folgende Person ist ☒ Anwalt ☐ gemeinsamer Vertreter

und ☒ ist vom (von den) Anmelder(n) bereits früher bestellt worden und vertritt ihn (sie) auch für die internationale vorläufige Prüfung.

☐ wird hiermit bestellt; eine etwaige frühere Bestellung eines Anwalts/gemeinsamen Vertreters wird hiermit widerrufen.

☐ wird hiermit zusätzlich zu dem bereits früher bestellten Anwalt/gemeinsamen Vertreter, nur für das Verfahren vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde bestellt.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

JOSTARNDT, Hans-Dieter
Eupener Straße 266

52076 Aachen
Deutschland

Telefonnr.:
(++49)241/543213

Telefaxnr.:
(++49)241/543240

Fernschreibnr.:

☐ Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben wird.

Feld Nr. IV ERKLÄRUNG BETREFFEND ÄNDERUNGEN

Der Anmelder wünscht, daß die mit der internationalen vorläufigen Prüfung beauftragte Behörde*

i) ☒ die internationale vorläufige Prüfung auf der Grundlage der internationalen Anmeldung in der ursprünglich eingereichten Fassung aufnimmt.

ii) ☐ die Änderungen nach Artikel 34

☐ der Beschreibung (Änderungen liegen bei)

☐ der Ansprüche (Änderungen liegen bei)

☐ der Zeichnungen (Änderungen liegen bei)

berücksichtigt.

iii) ☐ die beim Internationalen Büro eingereichten Änderungen der Ansprüche nach Artikel 19 berücksichtigt (Kopie liegt bei).

iv) ☐ die Änderungen der Ansprüche nach Artikel 19 nicht berücksichtigt, sondern als überholt ansieht.

v) ☐ den Beginn der internationalen vorläufigen Prüfung bis zum Ablauf von 20 Monaten ab dem Prioritätsdatum aufschiebt, sofern die Behörde nicht eine Kopie nach Artikel 19 vorgenommener Änderungen oder eine Erklärung des Anmelders erhält, daß er keine solchen Änderungen vornehmen will (Regel 69.1 d)). *(Dieses Kästchen darf nur angekreuzt werden, wenn die Frist nach Artikel 19 noch nicht abgelaufen ist.)*

* Wenn kein Kästchen angekreuzt wird, wird mit der internationalen vorläufigen Prüfung auf der Grundlage der internationalen Anmeldung in der ursprünglich eingereichten Fassung begonnen; wenn eine Kopie der Änderungen der Ansprüche nach Artikel 19 und/oder Änderungen der internationalen Anmeldung nach Artikel 34 bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde eingeht, bevor diese mit der Erstellung eines schriftlichen Bescheids oder des internationalen vorläufigen Prüfungsberichts begonnen hat, wird jedoch die geänderte Fassung verwendet.

Feld Nr. V BENENNUNG VON STAATEN ALS AUSGEWÄHLTE STAATEN

☒ Der Anmelder benennt als ausgewählte Staaten alle auswählbaren Staaten *(das heißt, alle Staaten, die bestimmt wurden und durch Kapitel II des PCT gebunden sind)* ausgenommen .....

.....

.....

.....

(Möchte der Anmelder bestimmte Staaten nicht auswählen, sind die Namen oder Zweibuchstaben-Codes dieser Staaten auf den obenstehenden Zeilen anzugeben.)

Blatt Nr. 3.....

Internationales Aktenzeichen
PCT/DE00/03507

Feld Nr. VI KONTROLLISTE

Dem Antrag liegen folgende Unterlagen für die Zwecke der internationalen vorläufigen Prüfung bei:			Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen: erhalten	nicht erhalten
1. Änderungen nach Artikel 34				
Beschreibung	:	Blätter	☐	☐
Ansprüche	:	Blätter	☐	☐
Zeichnungen	:	Blätter	☐	☐
2. Begleitschreiben zu den Änderungen nach Artikel 34	:	Blätter	☐	☐
3. Kopie der Änderungen nach Artikel 19	:	Blätter	☐	☐
4. Kopie einer Erklärung nach Artikel 19	:	Blätter	☐	☐
5. Sonstige *(einzeln aufführen)*:	:	Blätter	☐	☐

Dem Antrag liegen außerdem die nachstehend angekreuzten Unterlagen bei:

1. ☐ unterzeichnete gesonderte Vollmacht
2. ☐ Kopie der allgemeinen Vollmacht
3. ☐ Begründung für das Fehlen der Unterschrift
4. ☒ Blatt für die Gebührenberechnung
5. ☐ sonstige *(einzeln aufführen)*:

Feld Nr. VII UNTERSCHRIFT DES ANMELDERS, ANWALTS ODER GEMEINSAMEN VERTRETERS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Hans-Dieter Jostarndt

JOSTARNDT, Hans-Dieter
- Patentanwalt -
European Patent Attorney, No.: 093250

Aachen, 02. Mai 2001

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

1. Datum des tatsächlichen Eingangs des ANTRAGS:
2. Geändertes Eingangsdatum des Antrags aufgrund von BERICHTIGUNGEN nach Regel 60.1.b):
3. ☐ Eingangsdatum des Antrags NACH Ablauf von 19 Monaten ab Prioritätsdatum; Punkt 4 und Punkt 5, unten, finden keine Anwendung. ☐ Der Anmelder wurde entsprechend unterrichtet
4. ☐ Eingangsdatum des Antrags INNERHALB 19 Monate ab Prioritätsdatum wegen Fristverlängerung nach Regel 80.5.
5. ☐ Das Eingangsdatum des Antrags liegt nach Ablauf von 19 Monaten ab Prioritätsdatum, der verspätete Eingang ist aber nach Regel 82 ENTSCHULDIGT.

Vom Internationalen Büro auszufüllen

Antrag vom IPEA erhalten am:

KAPITEL II

PCT

BLATT FÜR DIE GEBÜHRENBERECHNUNG

Anlage zum Antrag auf internationale vorläufige Prüfung

Internationales Aktenzeichen	PCT/DE00/03507
Aktenzeichen des Anmelders oder Anwalts	ACDPA5003PWO

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

Eingangsstempel der IPEA

Anmelder DEUTSCHE POST AG, Heinrich-von-Stephan-Straße 1, D-53175 Bonn

Berechnung der vorgeschriebenen Gebühren

1. Gebühr für die vorläufige Prüfung	2998,29	P
2. Bearbeitungsgebühr *(Anmelder aus einigen Staaten haben Anspruch auf eine Ermäßigung der Bearbeitungsgebühr um 75%. Hat der Anmelder (oder haben alle Anmelder) einen solchen Anspruch, so beträgt der in Feld H einzutragende Betrag 25 % der Bearbeitungsgebühr.)*	287,51	H
3. Gesamtbetrag der vorgeschriebenen Gebühren Addieren Sie die Beträge in den Feldern P und H und tragen Sie die Summe in das nebenstehende Feld ein	3285,80	INSGESAMT

Zahlungsart

- ☐ Abbuchungsauftrag für das laufende Konto bei der IPEA (siehe unten)
- ☐ Scheck
- ☐ Postanweisung
- ☐ Bankwechsel
- ☐ Barzahlung
- ☐ Gebührenmarken
- ☐ Kupons
- ☒ Sonstige *(einzeln angeben):* Überweisung

Abbuchungsauftrag *(diese Zahlungsweise gibt es nicht bei allen Behörden)*

Die IPEA/ ____

☐ wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen.

☐ *(dieses Kästchen darf nur angekreuzt werden, wenn die Vorschriften der IPEA über laufende Konten dieses Verfahren erlauben)* wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben.

Kontonummer ____ Datum *(Tag/Monat/Jahr)* ____ Unterschrift ____

Siehe Anmerkungen zum Blatt für die Gebührenberechnung

Neue Patentansprüche:

1. Verfahren zur Erstellung fälschungssicherer Dokumente oder Datensätze unter Einsatz eines Sicherungsmoduls,
- wobei das Sicherungsmodul ein Geheimnis erzeugt, das einem Dokumenthersteller nicht zur Kenntnis gelangt,
- wobei das Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird,
- wobei die Bescheinigungsstelle das Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das Geheimnis zusammen mit Informationen zur Identität des Dokumentherstellers derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann, und an den Dokumenthersteller übermittelt,
- wobei der Dokumenthersteller eigene Daten dem Sicherungsmodul übergibt,
- wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten mit dem Geheimnis irreversibel verknüpft und
- wobei keine Rückschlüsse auf das Geheimnis möglich sind,

d a d u r c h g e k e n n z e i c h n e t, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem Geheimnis, die von dem Dokumenthersteller selbst eingebrachten Daten sowie die verschlüsselten Informationen der Bescheinigungsstelle das Dokument bilden, das an die Prüfstelle übermittelt wird.

2. Verfahren nach Anspruch 1, d a d u r c h g e k e n n - z e i c h n e t, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen Angaben zur Identität des Dokumentherstellers und zum Gültigkeitszeitraum der von dem Dokumenthersteller hergestellten Dokumente enthält.

3. Verfahren zur Überprüfung der Echtheit eines Dokuments, d a d u r c h g e k e n n z e i c h - n e t, dass die Prüfungsstelle überprüft, ob ein Ergebnis einer irreversiblen Verknüpfung aus von einem Dokumenthersteller eingebrachten Daten und einem Geheimnis in das Dokument übernommen wurde, indem die Prüfstelle das Geheimnis und weitere Informationen, die von einer Bescheinigungsstelle verschlüsselt wurden, entschlüsselt, dass die Prüfstelle in derselben Weise wie ein zur Herstellung des fälschungssicheren Dokuments eingesetztes Sicherungsmodul die von dem Dokumenthersteller in das Dokument eingebrachten Daten mit dem entschlüsselten Geheimnis irreversibel verknüpft und dass die Prüfstelle das Ergebnis der selbst durchgeführten irreversiblen Verknüpfung mit einem Ergebnis einer von dem Dokumenthersteller durchgeführten irreversiblen Verknüpfung vergleicht, die in das Dokument übernommen wurde.

4. Verfahren nach Anspruch 3, d a d u r c h g e k e n n z e i c h n e t, dass durch den Vergleich ermittelt wird, ob in das Dokument von dem Dokumenthersteller eingebrachte Daten verfälscht wurden.

REPLACED BY ART 34 AMDT

Patent Claims

1. A method for producing forgery-proof documents using a security module,
   - whereby the security module generates a temporary secret which remains unknown to a document producer,
   - whereby the temporary secret, together with information that reveals details about the identity of the security module, is transferred in encrypted form to an authentication unit,
   - whereby an authentication unit decrypts the temporary secret, recognizes the identity of the security module and encrypts the temporary secret, together with additional information, in such a way that only a checking unit can carry out a decryption and then the authentication unit transmits the temporary secret and the additional information to the document producer,
   - whereby the document producer transfers its own data, which has been introduced into the document, to the security module,
   - whereby the security module irreversibly links the temporary secret with the data that the document producer itself has introduced in such a way that only when the same data is linked again in the same manner can an identical result be obtained, and
   - whereby it is not possible to draw conclusions about the temporary secret,

   characterized in that the result of the irreversible linking of the temporary secret with the data introduced by the document producer is incorporated into the document.

2. The method according to Claim 1, **characterized in that** the additional information transferred by the authentication unit, together with the temporary secret, is transmitted in encrypted form to the document producer.

3. The method according to Claim 2, **characterized in that** the additional

information transferred by the authentication unit, which is transmitted to the document producer, together with the temporary secret, is transmitted in such a way that only a checking unit can carry out a decryption.

4. The method according to one or more of the preceding claims, **characterized in that** the additional information transferred by the authentication unit contains details on the identity of the document producer and on the validity of the documents generated by the document producer.

5. The method for checking the authenticity of a document, **characterized in that** the checking unit checks whether the result of an irreversible linking of a secret with data introduced by a document producer have been incorporated into the document, in that the checking unit decrypts the secret and additional information that were encrypted by an authentication unit, and in that the checking unit irreversibly links the decrypted temporary secret with the data introduced into the document by the document producer, in the same manner as a security module used to produce the forgery-proof document.

6. The method according to Claim 5, **characterized in that** the checking unit compares the result of the irreversible linking that it has performed itself with the result of an irreversible linking that was performed by the document producer and incorporated into the document.

7. The method according to Claim 6, **characterized in that** the comparison determines whether data introduced into the document by the document producer has been forged.

8. A method for producing and later checking forgery-proof documents, **characterized in that** the documents are produced by a method according to one or more of Claims 1 to 4, and in that the documents are subsequently checked by means of a method according to one or more of Claims 5 to 7.

9. The method according to Claim 8, **characterized in that** there is no direct communication and no shared data storage and data processing between the authentication unit and the checking unit.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
12. April 2001 (12.04.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/25880 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/DE00/03507

(22) Internationales Anmeldedatum:
5. Oktober 2000 (05.10.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 48 319.1 7. Oktober 1999 (07.10.1999) DE
100 20 563.1 27. April 2000 (27.04.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: DEUTSCHE POST AG [DE/DE]; Heinrich-von-Stephan-Strasse 1, 53175 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: LANG, Jürgen [DE/DE]; Schau ins Land 15, 51429 Bergisch Gladbach (DE). MEYER, Bernd [DE/DE]; Zum Stöckerhof 2 c, 53639 Königswinter (DE).

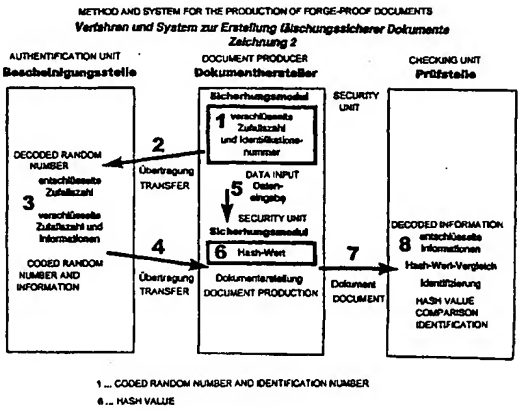
(74) Anwalt: JOSTARNDT, Hans-Dieter; Eupener Strasse 266, 52076 Aachen (DE).

(81) Bestimmungsstaaten *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR PRODUCING AND CHECKING FORGE-PROOF DOCUMENTS

(54) Bezeichnung: VERFAHREN ZUR ERSTELLUNG UND ÜBERPRÜFUNG FÄLSCHUNGSSICHERER DOKUMENTE



(57) Abstract: The invention relates to a method for producing forge-proof documents using a security module, whereby the security module generates a temporary secret which is unknown to the document producer. The temporary secret, in conjunction with information revealed about the identity of the security module, is transferred in encrypted form to an authentication unit. Said authentication unit decodes the temporary secret, recognizes the identity of the security module and the temporary secret together with other information which is coded in such a way that only one checking station can implement decoding and transfer said temporary secret to the document producer. The document producer transfers producer data, which is integrated into the document, to the security module. The data introduced into the security module by said document producer is irreversibly linked with the temporary secret in such a way that repeated linking of the same data in the same manner yields an identical result. It is not possible to draw conclusions about the temporary secret. The inventive method is characterized in that the result of the irreversible linking of data introduced by said document producer can be introduced into said document together with said temporary secret. The invention also relates to a method for checking the authenticity of a given document.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls, wobei das Sicherungsmodul ein temporäres Geheimnis erzeugt, das einem Dokumentenhersteller nicht zur Kenntnis gelangt, wobei das temporäre Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls

[Fortsetzung auf der nächsten Seite]

WO 01/25880 A2

ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird, wobei eine Bescheinigungsstelle das temporäre Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das temporäre Geheimnis zusammen mit weiteren Informationen derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann und an den Dokumenthersteller übermittelt, wobei der Dokumenthersteller eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt, wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten in einer Weise mit dem temporären Geheimnis irreversibel verknüpft, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann und wobei keine Rückschlüsse auf das temporäre Geheimnis möglich sind. Erfindungsgemäss zeichnet sich dieses Verfahren dadurch aus, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem temporären Geheimnis in das Dokument übernommen wird. Die Erfindung betrifft ferner ein Verfahren zur Überprüfung der Echtheit eines Dokuments.

Beschreibung

Verfahren zur Erstellung und Überprüfung fälschungssicherer Dokumente

Die Erfindung betrifft ein Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls, wobei das Sicherungsmodul ein temporäres Geheimnis erzeugt, das einem Dokumenthersteller nicht zur Kenntnis gelangt, wobei das temporäre Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird, wobei eine Bescheinigungsstelle das temporäre Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das temporäre Geheimnis zusammen mit weiteren Informationen derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann und das verschlüsselte temporäre Geheimnis und die weiteren Informationen an den Dokumenthersteller übermittelt, wobei der Dokumenthersteller eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt, wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten in einer Weise mit dem temporären Geheimnis irreversibel verknüpft, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann und wobei keine Rückschlüsse auf das temporäre Geheimnis möglich sind.

Die Erfindung betrifft ferner ein Verfahren zur Überprüfung der Echtheit eines Dokuments.

An diesem Verfahren und diesem System, die die Funktionsweisen eines Sicherungsmoduls im Umfeld der digitalen Signatur und des Einsatzes von Verschlüsselungstechniken betreffen, sind neben dem Sicherungsmodul drei Parteien beteiligt:

- der Hersteller/Bearbeiter eines Dokuments, nachfolgend „Dokumentenhersteller" genannt,

- eine Bescheinigungsstelle, die das Sicherungsmodul identifizieren und mit der Identität des Dokumentherstellers verknüpfen kann und

- eine Prüfstelle, bei der die Prüfungen der Unverfälschtheit des Dokuments und der Identität des Dokumentherstellers stattfindet.

Zur Gewährleistung der Fälschungssicherheit von Dokumenten und zur Identifizierung von Dokumentherstellern sind Systeme zur digitalen Signatur wie etwa Public-Key-Signaturverfahren nach Patentschrift DE 195 13 896 A1 oder DE 197 03 929 A1 bekannt.

Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (vgl. SigG §2, Abs. 1). Unter Benutzung der hier verwandten Terminologie ist eine Prüfstelle in der Lage, die digitale Signatur eines Dokumentherstellers und somit sowohl dessen Identität als auch die Unverfälschtheit der im Dokument enthaltenen Daten zu prüfen, wenn ihr der

öffentliche Signaturschlüssel des Dokumentherstellers, der mit einem Signaturschlüssel-Zertifikat versehen ist, zur Verfügung steht.

Problematisch ist die Anwendung des Verfahrens der digitalen Signatur dann, wenn entweder der Prüfstelle nicht der öffentliche Signaturschlüssel des Dokumentherstellers, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehen ist, zur Verfügung steht oder der Dokumenthersteller keinen eigenen privaten oder öffentlichen Signaturschlüssel besitzt.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Erstellung und/oder Überprüfung fälschungssicherer Dokumente zu schaffen, das auch dann einsetzbar ist, wenn die Prüfstelle nicht den öffentlichen Signaturschlüssel des Dokumentherstellers kennt und/oder wenn der Dokumenthersteller keinen eigenen privaten oder öffentlichen Signaturschlüssel besitzt.

Erfindungsgemäss wird diese Aufgabe dadurch gelöst, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit dem temporären Geheimnis in das Dokument übernommen wird.

Gegenstand der Erfindung ist ferner, ein gattungsgemäßes Verfahren zum Überprüfen der Echtheit von Dokumenten so durchzuführen, dass die Prüfungsstelle überprüft, ob ein Ergebnis einer irreversiblen Verknüpfung aus von einem Dokumenthersteller eingebrachten Daten und einem Geheimnis in das Dokument übernommen wurde, indem die Prüfstelle das Geheimnis und weitere Informationen, die von einer Bescheinigungsstelle verschlüsselt wurden, entschlüsselt.

Hierbei ist es besonders vorteilhaft, dass die Prüfstelle in derselben Weise wie ein zur Herstellung des fälschungssicheren Dokuments eingesetztes Sicherungsmodul die von dem Dokumenthersteller in das Dokument eingebrachten Daten mit dem entschlüsselten temporären Geheimnis irreversibel verknüpft.

Zur Erhöhung der Datensicherheit bei der Erstellung der Dokumente ist es zweckmäßig, das Verfahren zur Erstellung der Dokumente so durchzuführen, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden.

Hierbei ist es besonders vorteilhaft, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen, die neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden, derart übermittelt werden, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann.

Zweckmässigerweise wird das Verfahren so durchgeführt, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen Angaben zur Identität des Dokumentherstellers und zur Gültigkeit der von dem Dokumenthersteller hergestellten Dokumente enthält.

Um zu überprüfen, ob die Dokumente nach dem zuvor beschriebenen Verfahren von dem dazu berechtigten Dokumenthersteller erzeugt wurden, ist es zweckmäßig, das Verfahren zur Überprüfung der Echtheit des Dokuments so durchzuführen, dass die Prüfstelle das Ergebnis der selbst durchgeführten irreversiblen Verknüpfung mit einem Ergebnis

einer von dem Dokumenthersteller durchgeführten irreversiblen Verknüpfung vergleicht, die in das Dokument übernommen wurde.

Hierbei ist es vorteilhaft, dass durch den Vergleich ermittelt wird, ob in das Dokument von dem Dokumenthersteller eingebrachte Daten verfälscht wurden.

Obwohl die Schritte des Herstellens und des Prüfens voneinander getrennt stattfinden, ist eine Verbindung zu einem Gesamtverfahren, bei dem sowohl die Erzeugung als auch die Prüfung der Dokumente nach zuvor festgelegten Kriterien erfolgen, besonders vorteilhaft.

Hierbei ist es zweckmäßig, dass keine unmittelbare Kommunikation und keine gemeinsame Datenhaltung und -verarbeitung zwischen der Bescheinigungs- und der Prüfstelle stattfindet.

Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen und der nachfolgenden Darstellung eines bevorzugten Ausführungsbeispiels anhand der Zeichnungen.

Von den Zeichnungen zeigt

Fig. 1 ein Sicherungsmodul, das in dem Verfahren eingesetzt werden kann und

Fig. 2 eine schematische Darstellung eines Systems zur Erzeugung und zur Überprüfung fälschungssicherer Dokumente.

Durch das hier beschriebene Verfahren und System ergibt sich

für eine Prüfstelle, bei der der Dokumenthersteller und das von ihm hergestellte Dokument nicht bekannt sind, die Möglichkeit, auch ohne Anwendung der digitalen Signatur durch den Dokumenthersteller die Unverfälschtheit der in dem Dokument enthaltenen Daten sowie der Identität des Dokumentherstellers zuverlässig zu prüfen.

Hierzu verwendet der Dokumenthersteller ein Sicherungsmodul, das unter Einsatz unterschiedlicher technischer Mittel, vorzugsweise unter Zusammenwirken von Software mit programmierbarer Hardware realisiert wird und 5 aktive und 3 passive Einheiten sowie 2 Datenausgänge und 1 Dateneingang enthält (vgl. Zeichnung 1).

Die aktiven Einheiten sind:

- ein Geheimnisgenerator, der ein nicht vorhersagbares, temporäres Geheimnis erzeugt (Zufallszahl),

- eine Verschlüsselungsmaschine, die nach bekannten Verfahren einen Eingangswert mit einem in einem Register gespeicherten Schlüssel verschlüsselt,

- eine Hash-Maschine, die nach einem bekannten Verfahren aus einem Eingangswert einen Hash-Wert dieses Eingangswerts bildet (vgl. SigV § 17, Abs. 2) und

- zwei Kombinationsmaschinen, die aus jeweils zwei Eingangswerten einen Ergebniswert zusammensetzen.

Die passiven Einheiten sind:

- ein Schlüsselregister, in dem ein Schlüssel gespeichert

ist, mit dem Verschlüsselungen erzeugt werden können, die nur von der Bestätigungsstelle entschlüsselt werden können,

- ein Identifikationsregister, in dem Dateien enthalten sind, mit denen sich das Sicherungsmodul bei einer Bestätigungsstelle eindeutig identifizieren kann und

- ein Zwischenspeicher, in dem das im Geheimnisgenerator erzeugte Geheimnis temporär gespeichert wird.

Die Dateneingänge und die Datenausgänge sind die einzigen richtungsspezifischen Eingabe- und Ausgabemöglichkeiten für das Sicherungsmodul. Eine andere Art des Zugriffs oder Zugangs zum Sicherungsmodul ist weder für den Dokumenthersteller noch für Dritte möglich. Im Einzelnen handelt es sich bei den Dateneingängen und Datenausgängen um:

- einen Datenausgang 1, durch den Daten ausgegeben werden, die an die Bescheinigungsstelle übertragen werden,

- einen Datenausgang 2, durch den Daten ausgegeben werden, die auf das Dokument übernommen werden und

- einen Dateneingang, durch den Informationen vom Dokumenthersteller in das Sicherungsmodul eingegeben werden können.

Vorzugsweise wird in dem Verfahren zur Erstellung der fälschungssicheren Dokumente das nachfolgend dargestellte Sicherungsmodul eingesetzt.

In dem Sicherungsmodul erzeugt ein Geheimnisgenerator ein nicht vorhersagbares Geheimnis (zum Beispiel eine

Zufallszahl), das außerhalb des Sicherungsmoduls unbekannt bleibt, und übergibt dieses Geheimnis einerseits an die Kombinationsmaschine 1 und andererseits an den Zwischenspeicher. Die Kombinationsmaschine 1 kombiniert das Geheimnis mit den im Identifikationsregister enthaltenen Daten, die das Sicherungsmodul bei einer Bestätigungsstelle eindeutig identifizieren. Der Ergebniswert der Kombinationsmaschine wird in die Verschlüsselungsmaschine eingegeben, die mit dem Schlüssel aus dem Schlüsselregister einen verschlüsselten Ergebniswert erzeugt, der nur von der Bescheinigungsstelle entschlüsselt werden kann. Dieser Ergebniswert wird aus dem Datenausgang 1 aus dem Sicherungsmodul ausgegeben, um an die Bescheinigungsstelle übertragen zu werden.

Entschlüsselt die Bescheinigungsstelle den aus Datenausgang 1 ausgelassenen und übertragenen Ergebniswert, zerlegt sie diesen Ergebniswert in das Geheimnis und die Daten aus dem Identifikationsregister, identifiziert das Sicherungsmodul anhand der Daten aus dem Identifikationsregister und verschlüsselt das Geheimnis und weitere Informationen mit einem Schlüssel, der nur von der Prüfstelle entschlüsselt werden kann, so können das verschlüsselte Geheimnis und weitere Informationen an den Dokumenthersteller übertragen, von diesem auf das Dokument übernommen und von der Prüfstelle entschlüsselt werden.

Daten, die der Dokumenthersteller selbst über den Dateneingang in das Sicherungsmodul einbringt, werden von der Kombinationsmaschine 2 mit dem im Zwischenspeicher gespeicherten Geheimnis kombiniert. Der Ergebniswert der Kombinationsmaschine 2 wird in die Hash-Maschine eingegeben, die nach einem bekannten Verfahren einen Hash-Wert des

eingegebenen Wertes bildet. Dieser Ergebniswert wird aus dem Datenausgang 2 aus dem Sicherungsmodul ausgegeben, um in das Dokument übernommen zu werden.

In das Dokument übernommen werden vorzugsweise:

- diejenigen Daten, die der Dokumenthersteller selbst über den Dateneingang in das Sicherungsmodul eingebracht hat,

- der durch Datenausgang 2 aus dem Sicherungsmodul ausgegebene Hash-Wert und

- das von der Bescheinigungsstelle verschlüsselte Geheimnis und weitere Informationen, die nur von der Prüfstelle entschlüsselt werden können.

Eine Prüfstelle führt die Prüfung der Unverfälschtheit des Dokuments und der Identität des Dokumentherstellers durch, indem das von der Bescheinigungsstelle verschlüsselte Geheimnis und weitere Informationen entschlüsselt werden, nach einem bekannten Verfahren ebenso wie im Sicherungsmodul ein Hash-Wert aus einer Kombination aus den vom Dokumenthersteller selbst eingebrachten Daten und dem Geheimnis gebildet wird und dieser Hash-Wert mit dem übermittelten Hash-Wert verglichen wird. Ergibt der Vergleich der Hash-Werte - analog zur Prüfung einer digitalen Signatur - eine Identität des erzeugten und des übermittelten Hash-Wertes, so kann das Dokument nicht verfälscht worden sein.

Von der Bescheinigungsstelle werden weitere Informationen derart verschlüsselt an den Dokumenthersteller übermittelt, dass nur die Prüfstelle sie entschlüsseln kann, und die an den Dokumenthersteller zur Übernahme in das fälschungssichere

Dokument übermittelt werden, um Informationen zur Identität des Dokumentherstellers und zum Gültigkeitszeitraum der vom Dokumentenhersteller hergestellten Dokumente.

Ein bevorzugtes Einsatzgebiet der Erfindung besteht darin, dass Dokumenthersteller beispielsweise solche Personen sind, die über einen Computer (PC) Dokumente wie beispielsweise Eintrittskarten, Flugtickets oder Gutscheine selbst ausdrucken, deren Unverfälschtheit von einer Prüfstelle, die beispielsweise den entsprechenden Eintritt regelt, verifiziert werden kann. Die Bescheinigungsstelle ist beispielsweise die Ausgabestelle der Eintrittskarten, mit der der Dokumenthersteller im Vorfeld des Ausdrucks der Eintrittskarten auf elektronischem Weg über das Internet kommuniziert. Das Sicherungsmodul ist ein technisches Mittel, das vorzugsweise unter Zusammenwirken von Software mit programmierbarer Hardware realisiert wird und zumindest temporär Bestandteil der Hard- und Software des PC des Dokumentherstellers ist.

Die Erfindung kann sicherstellen, dass beispielsweise die den Eintritt regelnde Prüfstelle auch ohne Prüfung der digitalen Signatur des Dokumentherstellers mit all den hieraus erwachsenen Konsequenzen (individuelle öffentliche Signaturschlüssel aller zu prüfenden Dokumenthersteller) die Unverfälschtheit eines Dokuments verifizieren kann, das im Einflußbereich eines nicht vertrauenswürdigen Dokumentherstellers über dessen PC und Drucker erstellt wurde. Das Sicherungsmodul gewährleistet dabei die Unverfälschbarkeit von Informationen, die vom Dokumenthersteller ohne Kenntnis der Bescheinigungsstelle in das Dokument eingefügt wurden, sowie die Identifizierbarkeit des Dokumentherstellers.

Vorteilhafte Wirkungen dieser Erfindung sind darin zu sehen, dass Firmen und Organisationen ihren Kunden durch den Einsatz von Sicherungsmodulen die Möglichkeit geben können, einfach über das Internet den Ausdruck von Dokumenten zu erlauben, deren Unverfälschtheit zweifelsfrei geprüft werden kann. Besonders vorteilhaft ist hierbei der Verzicht auf den Einsatz digitaler Signaturen durch den Dokumenthersteller, der mit einem erheblichen infrastrukturellen, organisatorischen Aufwand und einer landesspezifischen Rechtsunsicherheit einhergeht. Weiterhin ist es bei dem beschriebenen Verfahren und System vorteilhaft, dass der Umfang derjenigen Informationen, die innerhalb des Dokuments der Prüfung durch die Prüfstelle dienen, im Vergleich zur digitalen Signatur, bei der der öffentliche, mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle versehene Signaturschlüssel des Dokumentherstellers einen Teil des Dokuments darstellen kann, sehr gering ist. Vorteilhaft ist weiterhin, dass zur Prüfung der Unverfälschtheit keine unmittelbare Kommunikation und keine gemeinsame Datenhaltung und -verarbeitung zwischen Bescheinigungs- und Prüfstelle stattfinden muss. Vorteilhaft ist schließlich, dass eine grundsätzliche Entkopplung zwischen der Kommunikation zwischen dem Sicherungsmodul und der Bescheinigungsstelle einerseits und der Dokumentherstellung und -prüfung andererseits in der Art erfolgen kann, dass mehrere Dokumente auf Basis einer Kommunikation zwischen Sicherungsmodul und Bescheinigungsstelle hergestellt werden können, in die vom Dokumenthersteller unterschiedliche dokumentspezifische Daten eingegeben werden können.

Ein zweckmässiges Verfahren zur Erzeugung und Prüfung

fälschungssicherer Dokumente wird nachfolgend anhand von Fig.2 dargestellt.

In Fig. 2 ist ein System dargestellt, in dem von einem Dokumenthersteller erzeugte Informationen an eine Bescheinigungsstelle übertragen, dort verarbeitet und erneut an den Dokumenthersteller übertragen werden. Der Dokumenthersteller stellt unter Verwendung der von der Bescheinigungsstelle übermittelten Informationen fälschungssichere Dokumente her. Ein von der Dokumentenherstellung vorzugsweise getrennter Vorgang ist eine Prüfung der fälschungssicheren Dokumente in einer Prüfstelle.

Das dargestellte System beinhaltet die nachfolgend dargestellten Prozessschritte 1 bis 8.

In einem ersten Prozessschritt 1 erfolgt die Erzeugung eines temporären Geheimnisses in Form einer Zufallszahl, die zusammen mit einer Identifikationsnummer des Sicherungsmoduls mit dem öffentlichen Schlüssel der Bescheinigungsstelle verschlüsselt wird, so dass dieses temporäre Geheimnis dem Dokumenthersteller nicht zur Kenntnis gelangen kann und nur von der Bescheinigungsstelle entschlüsselt werden kann.

In dem mit dem Bezugszeichen 2 gekennzeichneten Prozessschritt erfolgt die Übertragung der verschlüsselten Zufallszahl und Identifikationsnummer zur Bescheinigungsstelle. Zu beachten ist, dass diese Übertragung auch über einen unsicheren Weg vonstatten gehen kann, da nur die Bescheinigungsstelle in der Lage ist, die Informationen zu entschlüsseln.

In einem anschliessenden Verfahrensschritt 3 erfolgt in der Bescheinigungsstelle die Entschlüsselung der Zufallszahl und der Identifikationsnummer mit dem privaten Schlüssel der Bescheinigungsstelle. Die Zufallszahl wird mit weiteren Informationen zur Identität des Dokumentherstellers zum Gültigkeitszeitraum der vom Dokumenthersteller hergestellten Dokumente derart verschlüsselt, dass nur die Prüfstelle die Zufallszahl und die weiteren Informationen entschlüsseln kann.

In dem mit dem Bezugszeichen 4 gekennzeichneten Verfahrensschritt erfolgt eine Übertragung der verschlüsselten Informationen zum Dokumenthersteller. Zu beachten ist, dass diese Übertragung auch über einen unsicheren Weg vonstatten gehen kann, da nur die Prüfstelle in der Lage sein wird, die Informationen zu entschlüsseln.

Aus diesem Grund eignet sich das Verfahren besonders für einen Einsatz in Datennetzen, die als solche gegen einen unbefugten Zugang nicht oder nur schwer gesichert werden können, wie dem Internet.

In dem mit dem Bezugszeichen 5 gekennzeichneten Verfahrensschritt gibt der Dokumenthersteller in das Sicherungsmodul eigene Daten ein, die zu einer Kennzeichnung des Dokuments dienen.

In dem mit dem Bezugszeichen 6 gekennzeichneten Verfahrensschritt erfolgt eine Bildung eines Hash-Wertes aus der Kombination von dem Dokumenthersteller eingegebenen Daten und der noch gespeicherten Zufallszahl. Das anschließend hergestellte Dokument enthält die Daten, die der Dokumenthersteller selbst in das Dokument einbringt, den

soeben gebildeten Hash-Wert sowie die verschlüsselten Informationen der Bescheinigungsstelle.

In einem weiteren Verfahrensschritt 7 erfolgt eine Übertragung des Dokuments, das aus den Daten des Benutzers, dem Hash-Wert und den verschlüsselten Informationen der Bescheinigungsstelle (vgl. Ziffer 3) besteht.

In einer Prüfstelle erfolgt in einem mit dem Bezugszeichen 8 gekennzeichneten Verfahrensschritt eine Entschlüsselung der Informationen der Bescheinigungsstelle mit dem Schlüssel der Prüfstelle. Nach Patentanspruch 1 kann die entschlüsselte Zufallszahl benutzt werden, um zusammen mit den Daten, die der Dokumenthersteller selbst in das Dokument eingebracht hat, einen Hash-Wert nach demselben, bekannten Verfahren zu bilden, das im Sicherungsmodul zur Bildung des Hash-Wertes benutzt wurde. Ein Vergleich des gebildeten Hash-Wertes mit dem übertragenen Hash-Wert gibt zuverlässige Auskunft darüber, ob die vom Dokumenthersteller selbst eingebrachten Daten verfälscht wurden. Nach Patentanspruch 2 können hierbei weitere Informationen zur Identität des Dokumentherstellers und zum Gültigkeitszeitraum der vom Dokumenthersteller hergestellten Dokumente entschlüsselt werden.

Durch das Verfahren und System zur Erstellung fälschungssicherer Dokumente unter Benutzung eines Sicherungsmoduls ergibt sich für eine Prüfstelle, bei der ein Dokumenthersteller und das von ihm hergestellte Dokument nicht bekannt sind, die Möglichkeit, auch ohne Anwendung der digitalen Signatur durch den Dokumenthersteller die Unverfälschtheit der in dem Dokument enthaltenen Daten sowie die Identität des Dokumentherstellers zuverlässig zu prüfen. Alle hierzu erforderlichen Prüfinformationen, die in das

Dokument zu übernehmen sind, werden von einer Bescheinigungsstelle zur Verfügung gestellt, mit der das beim Dokumenthersteller betriebene Sicherungsmodul im Vorfeld der Herstellung/Bearbeitung des Dokuments kommuniziert. Das Verfahren und System eignet sich insbesondere, um Personen die Möglichkeit zu geben, beispielsweise Eintrittskarten oder Gutscheine über den eigenen PC auszudrucken, die zweifelsfrei auf Unverfälschtheit geprüft werden können.

Patentansprüche:

1. Verfahren zur Erstellung fälschungssicherer Dokumente unter Einsatz eines Sicherungsmoduls,
   - wobei das Sicherungsmodul ein temporäres Geheimnis erzeugt, das einem Dokumenthersteller nicht zur Kenntnis gelangt,
   - wobei das temporäre Geheimnis zusammen mit Informationen, die Auskunft über die Identität des Sicherungsmoduls geben, verschlüsselt an eine Bescheinigungsstelle übergeben wird,
   - wobei eine Bescheinigungsstelle das temporäre Geheimnis entschlüsselt, die Identität des Sicherungsmoduls erkennt und das temporäre Geheimnis zusammen mit weiteren Informationen derart verschlüsselt, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann und das temporäre Geheimnis und die weiteren Informationen an den Dokumenthersteller übermittelt,
   - wobei der Dokumenthersteller eigene Daten, die in das Dokument eingebracht werden, dem Sicherungsmodul übergibt,
   - wobei das Sicherungsmodul die selbst vom Dokumenthersteller eingebrachten Daten in einer Weise mit dem temporären Geheimnis irreversibel verknüpft, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entstehen kann und
   - wobei keine Rückschlüsse auf das temporäre Geheimnis möglich sind,

   d a d u r c h g e k e n n z e i c h n e t, dass das Ergebnis der irreversiblen Verknüpfung der von dem Dokumenthersteller eingebrachten Daten mit

dem temporären Geheimnis in das Dokument übernommen wird.

2. Verfahren nach Anspruch 1, d a d u r c h g e k e n n z e i c h n e t, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden.

3. Verfahren nach Anspruch 2, d a d u r c h g e k e n n z e i c h n e t, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen, die neben dem temporären Geheimnis verschlüsselt an den Dokumenthersteller übermittelt werden, derart übermittelt werden, dass nur eine Prüfstelle eine Entschlüsselung vornehmen kann.

4. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, d a d u r c h g e k e n n z e i c h n e t, dass die von der Bescheinigungsstelle übergebenen weiteren Informationen Angaben zur Identität des Dokumentherstellers und zur Gültigkeit der von dem Dokumenthersteller hergestellten Dokumente enthält.

5. Verfahren zur Überprüfung der Echtheit eines Dokuments, d a d u r c h g e k e n n z e i c h n e t, dass die Prüfstelle überprüft, ob ein Ergebnis einer irreversiblen Verknüpfung aus von einem Dokumenthersteller eingebrachten Daten und einem Geheimnis in das Dokument übernommen wurde, indem die Prüfstelle das Geheimnis und weitere Informationen, die von einer Bescheinigungsstelle verschlüsselt wurden,

entschlüsselt, und dass die Prüfstelle in derselben Weise wie ein zur Herstellung des fälschungssicheren Dokuments eingesetztes Sicherungsmodul die von dem Dokumenthersteller in das Dokument eingebrachten Daten mit dem entschlüsselten temporären Geheimnis irreversibel verknüpft.

6. Verfahren nach Anspruch 5, d a d u r c h g e k e n n z e i c h n e t, dass die Prüfstelle das Ergebnis der selbst durchgeführten irreversiblen Verknüpfung mit einem Ergebnis einer von dem Dokumenthersteller durchgeführten irreversiblen Verknüpfung vergleicht, die in das Dokument übernommen wurde.

7. Verfahren nach Anspruch 6, d a d u r c h g e k e n n z e i c h n e t, dass durch den Vergleich ermittelt wird, ob in das Dokument von dem Dokumenthersteller eingebrachte Daten verfälscht wurden.

8. Verfahren zur Erstellung und zur späteren Überprüfung von fälschungssicheren Dokumenten, d a d u r c h g e k e n n z e i c h n e t, dass die Dokumente in einem Verfahren nach einem oder mehreren der Ansprüche 1 bis 4 erzeugt werden und dass die Dokumente anschließend nach einem Verfahren nach einem oder mehreren der Ansprüche 5 bis 7 überprüft werden.

9. Verfahren nach Anspruch 8, d a d u r c h g e k e n n z e i c h n e t, dass keine unmittelbare Kommunikation und keine gemeinsame Datenhaltung und -verarbeitung zwischen der Bescheinigungs- und der Prüfstelle stattfindet.

METHOD FOR PRODUCING AND CHECKING FORGE-PROOF DOCUMENTS

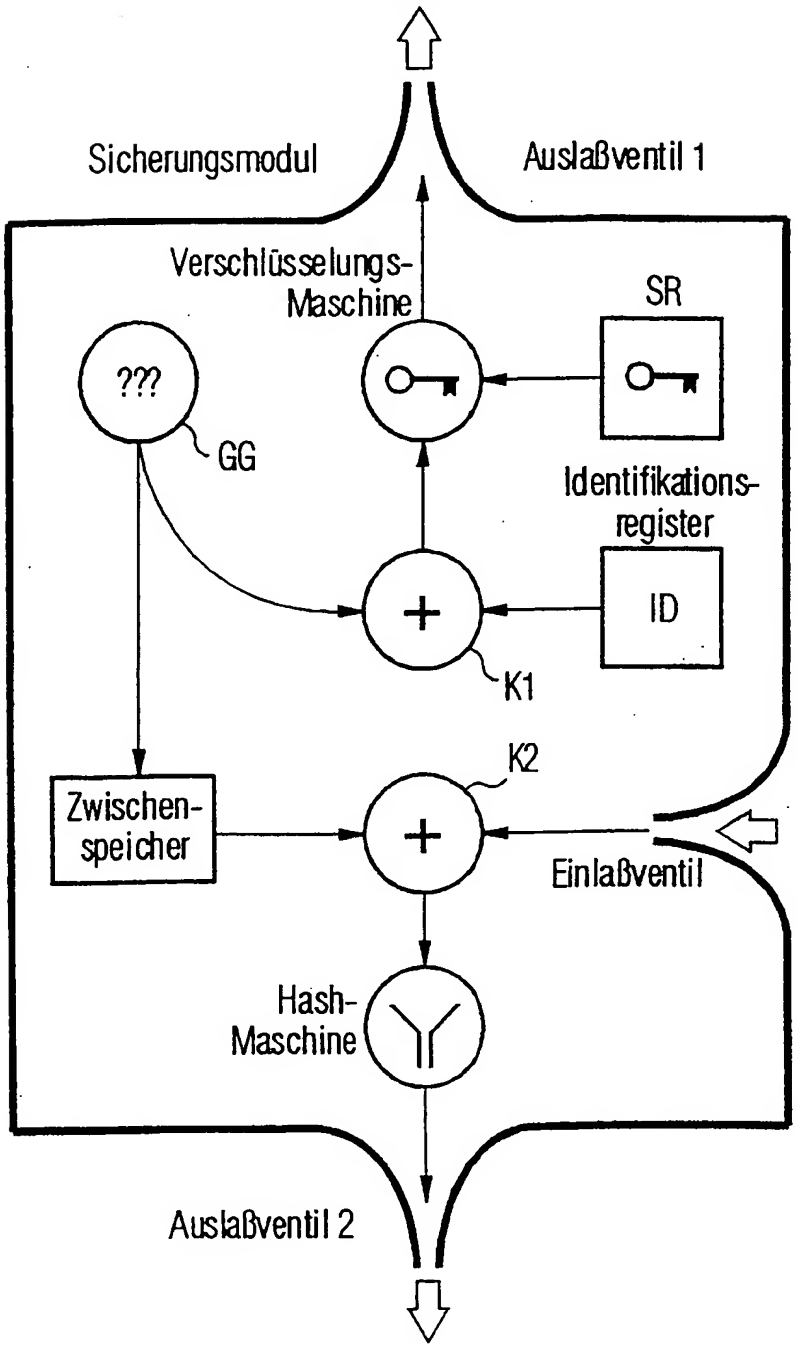
Jürgen Lang
-and-
Bernd Meyer

INTERNATIONAL APPLICATION
-with-
Search Report
-and-
Two (2) Sheets of Drawings
for

PCT/DE00/03507 .... IFD: -October 05, 2000-

ACDPA-5003 PWO .... (10096*2)
(POST-2)

Verfahren und System zur Erstellung
fälschungssicherer Dokumente
Zeichnung 1



Verfahren und System zur Erstellung fälschungssicherer Dokumente
Zeichnung 2